UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,397	02/17/2004	Matthew J. Wagner	200314073-1	1613

22879 7590 02/07/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ABBASZADEH, JAWEED A	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,397	WAGNER ET AL.	
	Examiner	Art Unit	
	Jaweed A. Abbaszadeh	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/17/2004 and 9/23/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claim 34 is objected to because of the following informalities: Line 1 of the claim states, "security model." It is suggested that this be changed to, "security module." Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-24 and 37-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Libin et al. (US 2005/0044386) in view of Bivens et al. (US 2003/0226036).

2. As to claim 1, Libin et al. teaches a computer security system (See Figure 1A, elements 24-26 are electronic devices that can be computers, See [0019]) comprising: a self-managed device (e.g. electronic device, See [0011]) having an authentication system for controlling access (e.g. validation unit, See [0045]) to the self-managed device (e.g. electronic device, See [0011]) by a user (e.g. users, See [0012]); and a security module adapted to authenticate an identity of the user (e.g. administrative entity...credentials include an identifier for a user, See [0011]), and device credential

data (e.g. generates the credentials, See [0011]) verifiable by the authentication system to enable user access (e.g. controller receiving credentials, determining if access is authorized, See [0011]) to the self-managed device (e.g. electronic device, See [0011]). It is noted that Libin does not specifically mention in response to user authentication, automatically generate, transparently to the user, device credential data. It would have been obvious to interpret that the credentials were generated transparent to the user because the reference does not state that the credentials are made available to the user. The reference only states that the credentials are created and stored (See [0037]). Bivens et al. is cited to teach a similar user authentication method. Bivens further teaches **in response to user authentication** (e.g. once user is authenticated, See [0037]), automatically generate device credential data (e.g. user credentials are created, See [0037]). It would have been obvious to one of ordinary skill in the art to modify Libin with the feature of generating credential data **in response to user authentication** as taught by Bivens because the credential data allows access for multiple applications which require independent authentication (Bivens, See [0012]).

3. As to claim 2, Libin et al. teaches the system of Claim 1, wherein the security module is adapted to randomly generate the device credential data to the self-managed device (e.g. random value is used...with generating the credentials, See [0054]).

4. As to claim 3, Libin et al. teaches the system of Claim 1, wherein the security module is adapted to automatically transmit the device credential data to the self-managed device (e.g. providing credentials, See [0021]). Libin does not specifically mention that the credential data is transmitted transparently to the user. It would have

been obvious to transmit the credentials transparently to the user because credentials are transmitted directly to the electronic device without any mention of transmitting to the user.

5. As to claim 4, Libin et al. teaches the system of Claim 1, wherein the security module is adapted to receive a request (e.g. receives a start signal, See [0045]) from a networked administration client (e.g. external interface, See Figure 2, 48) to activate the authentication system of the self-managed device (See [0045]).

6. As to claim 5, Libin et al. teaches the system of Claim 1, wherein the security module is disposed within a basic input/output system (BIOS) (e.g. BIOS, See [0038]).

7. As to claim 6, Libin et al. teaches the system of Claim 1, wherein the security module is adapted to access relational data correlating the user to the device credential data for the self-managed device (e.g. correlation generation data, See [0018]).

8. As to claim 7, Libin et al. teaches the system of Claim 1, further comprising an activation/deactivation module (e.g. proper entity E, See [0068]) accessible by an administration client (e.g. external interface, See Figure 2, 48) to activate the authentication system (See [0045]).

9. As to claim 8, Libin et al. teaches the system of Claim 1, further comprising an activation/deactivation module (e.g. proper entity E, See [0068]) accessible by an administration client (e.g. external interface, See Figure 2, 48) to deactivate the authentication system (e.g. stop issuing PROOFS of authorization; See [0069]).

10. As to claim 9, Libin et al. teaches the system of Claim 1, wherein the security module is adapted to receive a request from a networked administration client (e.g.

proper entity E, See [0068]) to deactivate the authentication system of the self-managed device (e.g. stop issuing PROOFS of authorization, See [0069]).

11. As to claim 10, Libin et al. teaches the system of claim 1, wherein the security module is adapted to perform a registration operation to register the self-managed device (e.g. identify the electronic device, See [0058]).

12. As to claim 11, Libin et al. teaches a computer security system (See Figure 1A, elements 24-26 are electronic devices that can be computers, See [0019]) comprising: means for controlling user access to a self-managed device (e.g. validation unit, See [0045]); and means for authenticating an identity of the user (e.g. administrative entity...credentials include an identifier for a user, See [0011]), and device credential data verifiable by the controlling means to enable user access (e.g. controller receiving credentials, determining if access is authorized, See [0011]) to the self-managed device (e.g. electronic device, See [0011]). It is noted that Libin does not specifically mention in response to user authentication, automatically generate, transparently to the user, device credential data. It would have been obvious to interpret that the credentials were generated transparent to the user because the reference does not state that the credentials are made available to the user. The reference only states that the credentials are created and stored (See [0037]). Bivens et al. is cited to teach a similar user authentication method. Bivens further teaches **in response to user authentication** (e.g. once user is authenticated, See [0037]), automatically generate device credential data (e.g. user credentials are created, See [0037]). It would have been obvious to one of ordinary skill in the art to modify Libin with the feature of

generating credential data **in response to authentication** as taught by Bivens because the credential data allows access for multiple applications which require independent authentication (Bivens, See [0012]).

13. As to claim 12, Libin et al. teaches the system of Claim 11, further comprising means for automatically transmitting device credential data, transparently to the user (It would have been obvious to transmit the credentials transparently to the user because credentials are transmitted directly to the electronic device without any mention of transmitting to the user), to the self-managed device (e.g. providing credentials, See [0021]) for verification by the controlling means (e.g. validation unit to examine credential data, See [0045]).

14. As to claim 13, Libin et al. teaches the system of Claim 11, further comprising means for correlating the device credential data with the user (e.g. correlation generation data, See [0018]).

15. As to claim 14, Libin et al. teaches the system of Claim 11 further comprising means for receiving a request (e.g. receives a start signal, See [0045]) from a networked administration client (e.g. external interface, See Figure 2, 48) to activate the authentication system of the self-managed device (See [0045]).

16. As to claim 15, Libin et al. teaches the system of Claim 11, further comprising means for randomly generating the device credential data (e.g. random value is used...with generating the credentials, See [0054]).

17. As to claim 16, Libin et al. teaches a computer security method, comprising: authenticating an identity of a user (e.g. administrative entity...credentials include an

identifier for a user, See [0011]) and device credential data verifiable by an authentication system (e.g. validation unit, See [0045]) of a self-managed device (e.g. electronic device, See [0011]) to enable user access to the self-managed device (e.g. controller receiving credentials, determining if access is authorized, See [0011]). It is noted that Libin does not specifically mention automatically generating transparently to the user, in response to user authentication, device credential data. It would have been obvious to interpret that the credentials were generated transparent to the user because the reference does not state that the credentials are made available to the user. The reference only states that the credentials are created and stored (See [0037]). Bivens et al. is cited to teach a similar user authentication method. Bivens further teaches **in response to user authentication** (e.g. once user is authenticated, See [0037]), automatically generate device credential data (e.g. user credentials are created, See [0037]). It would have been obvious to one of ordinary skill in the art to modify Libin with the feature of generating credential data **in response to authentication** as taught by Bivens because the credential data allows access for multiple applications which require independent authentication (Bivens, See [0012]).

18. As to claim 17, Libin et al. teaches the method of Claim 16, further comprising automatically transmitting, transparently to the user (It would have been obvious to transmit the credentials transparently to the user because credentials are transmitted directly to the electronic device without any mention of transmitting to the user), the device credential data to the self-managed device (e.g. providing credentials, See [0021]).

19. As to claim 18, Libin et al. teaches the method of Claim 16, further comprising randomly generating the device credential data (e.g. random value is used...with generating the credentials, See [0054]).

20. As to claim 19, Libin et al. teaches the method of Claim 16, further comprising receiving a request (e.g. receives a start signal, See [0045]) from a networked administration client (e.g. external interface, See Figure 2, 48) to activate the authentication system of the self-managed device (See [0045]).

21. As to claim 20, Libin et al. teaches the method of Claim 16, further comprising receiving a request from a networked administration client (e.g. proper entity E, See [0068]) to deactivate the authentication system of the self-managed device (e.g. stop issuing PROOFS of authorization, See [0069]).

22. As to claim 21, Libin et al. teaches the method of Claim 16, further comprising initiating an activation/deactivation module (e.g. proper entity E, See [0068]) to enable activation of the authentication system (e.g. causes the validation unit to examine credential data, See [0045]).

23. As to claim 22, Libin et al. teaches the method of Claim 16, further comprising accessing relational data correlating the device credential data with the user (e.g. correlation generation data, See [0018]).

24. As to claim 23, Libin et al. teaches the method of Claim 16, further comprising storing the device credential data at the self-managed device (e.g. electronic devices...credentials stored internally, See [0034]).

25. As to claim 24, Libin et al. teaches the method of Claim 16, further comprising performing a registration operation to register the self-managed device to the user (e.g. identify the electronic device, See [0058]).

26. As to claim 37, Libin et al. teaches a computer security method, comprising: authenticating an identity of a user (e.g. PIN or answer to a challenge, See [0012]) and authentication by the self-managed device to enable the user to access the self-managed device (e.g. controller receiving credentials, determining if access is authorized, See [0011]). It is noted that Libin does not specifically mention if the identity is successfully authenticated, transmitting transparently to the user, device credential data. It would have been obvious to transmit the credentials transparently to the user because credentials are transmitted directly to the electronic device without any mention of transmitting to the user. Bivens et al. is cited to teach a similar user authentication method. Bivens further teaches **in response to user authentication** (e.g. once user is authenticated, See [0037]), automatically generate device credential data (e.g. user credentials are created, See [0037]). It would have been obvious to one of ordinary skill in the art to modify Libin with the feature of generating credential data **in response to authentication** as taught by Bivens because the credential data allows access for multiple applications which require independent authentication (Bivens, See [0012]).

27. As to claim 38, Libin et al. teaches the method of Claim 37, further comprising correlating the identity of the user to the device credential data (e.g. correlation generation data, See [0018]).

28. As to claim 39, Libin et al. teaches the method of Claim 37, further comprising a registration operation to register the self-managed device (e.g. identify the electronic device, See [0058]).

29. As to claim 40, Libin et al. teaches the method of Claim 37, further comprising encrypting the device credential data (e.g. credentials may correspond to a digital certificate, See [0011]).

30. As to claim 41, Libin et al. teaches the method of Claim 37, wherein transmitting comprises transmitting (e.g. providing credentials, See [0021]), transparently to the user (It would have been obvious to transmit the credentials transparently to the user because credentials are transmitted directly to the electronic device without any mention of transmitting to the user), encrypted device credential data (e.g. credentials may correspond to a digital certificate, See [0011]) to the self-managed device for decryption by the self-managed device to authenticate access to the self-managed device (e.g. verifies the validity of the cert with the public key, See [0095]).

31. Claims 25-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Libin et al. (US 2005/0044386).

32. As to claim 25, Libin et al. teaches a computer security system (See Figure 1A, elements 24-26 are electronic devices that can be computers, See [0019]), comprising: a security module (e.g. administrative entity, See [0011]) executable by a processor (See [0200]), the security module adapted to access credential data to verify an identity of a user (e.g. administrative entity...credentials include an identifier for a user, See

[0011]); and an activation/deactivation module adapted to interface with the security module (e.g. second entity working for administrative entity, See [0068]) in response to a request by the administration client to activate an authentication system (e.g. causes the validation unit to examine credential data, See [0045]) of a self-managed device (e.g. electronic device, See [0011]) to control user access to the self-managed device (e.g. validation unit, See [0045]). It would have been obvious to activate the authentication system transparently to the user because the user need not be aware of the authentication process. The user should be excluded as much as possible in order to promote security User intervention is also not required making it unnecessary to alert the user of activating the authentication system.

33. As to claim 26, Libin et al. teaches the system of Claim 25, wherein the security module is adapted to automatically generate a device credential (e.g. generates the credentials, See [0011]) for verification by the authentication system (e.g. causes the validation unit to examine credential data, See [0045]). Libin does not specifically mention generating the credential transparently. It would have been obvious to interpret that the credentials were generated transparent to the user because the reference does not state that the credentials are made available to the user. The reference only states that the credentials are created and stored (See [0037]).

34. As to claim 27, Libin et al. teaches the system of Claim 25, wherein the security module is adapted to randomly generate, transparently to the user (It would have been obvious to interpret that the credentials were generated transparent to the user because the reference does not state that the credentials are made available to the user. The

reference only states that the credentials are created and stored (See [0037])), a device credential (e.g. random value is used...with generating the credentials, See [0054]) for verification by the authentication system (e.g. causes the validation unit to examine credential data, See [0045]).

35. As to claim 28, Libin et al. teaches the system of Claim 25, wherein the security module is adapted to transmit, transparently to the user (It would have been obvious to transmit the credentials transparently to the user because credentials are transmitted directly to the electronic device without any mention of transmitting to the user), a device credential to the device (e.g. providing credentials, See [0021]) for verification by the authentication system (e.g. causes the validation unit to examine credential data, See [0045]).

36. As to claim 29, Libin et al. teaches the system of Claim 25, wherein the activation/deactivation module is adapted to display to the user registered self-managed devices available for authentication (e.g. "device #123456 is valid," See [0058]).

37. As to claim 30, Libin et al. teaches the system of Claim 25, wherein the security module is adapted to correlate a device credential (e.g. correlation generation data, See [0018]) for verification by the authentication system with the user (e.g. causes the validation unit to examine credential data, See [0045]).

38. As to claim 31, Libin et al. teaches a computer (See Figure 1A, elements 24-26 are electronic devices that can be computers, See [0019]), network (e.g. LAN, WAN, Internet, See [0032] and also See Fig. 1A, 22) security system, comprising: a security module adapted to automatically generate device credential data (e.g. generates the

credentials, See [0011]) verifiable by an authentication system (e.g. validation unit, See [0045]) of a self-managed device (e.g. electronic device, See [0011]) to enable user access to the self-managed device (e.g. causes the validation unit to examine credential data, See [0045]); and an activation /deactivation module (e.g. proper entity E, See [0068]) adapted to receive a request from the user to automatically activate the authentication system of the self-managed device (e.g. receives a start signal, See [0045]). It is noted that Libin does not teach that the credential data is generated transparently. It would have been obvious to interpret that the credentials were generated transparent to the user because the reference does not state that the credentials are made available to the user. The reference only states that the credentials are created and stored (See [0037]).

39. As to claim 32, Libin et al. teaches the system of claim 31, wherein the security module is adapted to automatically transmit, transparently to the user (It would have been obvious to transmit the credentials transparently to the user because credentials are transmitted directly to the electronic device without any mention of transmitting to the user), the device credential data (e.g. providing credentials, See [0021]) to the authentication system (e.g. validation unit, See [0045]). It is interpreted that providing credentials to the electronic device also entails providing the credentials to the authentication system because it is part of the electronic device.

40. As to claim 33, Libin et al. teaches the system of claim 31, wherein the self-managed device is adapted to store the device credential data received from the security module (e.g. electronic devices...credentials stored internally, See [0034]).

41. As to claim 34, Libin et al. teaches the system of claim 31, wherein the security module is disposed within a basic input/output system (BIOS) (e.g. BIOS, See [0038]).

42. As to claim 35, Libin et al. teaches the system of claim 31, wherein the activation/deactivation module is adapted to receive a request from a networked administration client (e.g. external interface, See Figure 2, 48) to activate the authentication system (e.g. receives a start signal, See [0045]).

43. As to claim 36, Libin et al. teaches the system of claim 31, wherein the security module is adapted to randomly generate the device credential (e.g. random value is used...with generating the credentials, See [0054]).

Conclusion

44. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

45. Audebert (US 6,988,210) teaches a system which access is controlled by credentials.

46. Van Gunter et al. (US 7,039,713) teaches a user authentication process to allow access to a network.

47. Hashiguchi (US 6,615,353) teaches a user authentication method comprising control equipment and creates a user authentication code.

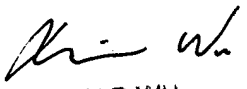
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaweed A. Abbaszadeh whose telephone number is

(571) 270-1640. The examiner can normally be reached on Mon-Fri: 7:30 a.m.-5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Xiao Wu can be reached on (571) 272-7761. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JA
1/24/2007



XIAO WU
SUPERVISORY PATENT EXAMINER